APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,547	06/20/2003	Masayuki Numao	JP920020102US1	6077

7590   07/06/2007

Louis P. Herzberg
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER
TOLENTINO, RODERICK

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>04 May 2007</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 19-21* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 19-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>20 June 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 10 and 19 – 21 are pending. Applicant canceled claims 11 – 18 and

22 – 25.

Specification

2.   The lengthy specification has not been checked to the extent necessary to

determine the presence of all possible minor errors. Applicant's cooperation is

requested in correcting any errors of which applicant may become aware in the

specification.

Response to Arguments

3.   Applicant's arguments with respect to claims 1 – 25, have been considered but

are moot in view of the new ground(s) of rejection, as necessitated by amendment by

applicant.

4.   Applicant's arguments with regards to 35 U.S.C. 112 2nd paragraph rejections

have been deemed persuasive and 112 2nd paragraph rejections have been withdrawn.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1, 3, 4, 6 – 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Matsumoto U.S. Patent No. (6,215,877) in view of Lerner et al. U.S.

Patent No. (6,169,802).

7.   As per claims 1, 20 and 21, Matsumoto teaches a key management server for

managing secret keys and public keys corresponding to given attribute values and a

provider terminal for generating an encrypted content that can be decrypted by said

user terminal having said attribute secret keys corresponding to given attributes by

means of said public keys (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5),

wherein said provider terminal distributes said encrypted content and said user terminal

decrypts said encrypted content decryptable by means of said attribute secret keys of

its own (Matsumoto, Col. 4 Lines 57 – 67) but fails to teach a user terminal for

accessing said key management server to obtain attribute secret keys generated based

on said secret keys, said attribute secret keys corresponding to attributes identifying

said user terminal. However, in an analogous art Lerner teaches a user terminal for

accessing said key management server to obtain attribute secret keys generated based

on said secret keys, said attribute secret keys corresponding to attributes identifying

said user terminal (Lerner, Col. 6 Lines 52 – 62).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Lerner's dynamic private key security with Matsumoto's

key management server and chat system because it offers the advantage of secure

messaging to secure privacy (Lerner, Col. 2 Lines 21 – 27).

8.   As per claim 3, Matsumoto teaches user terminal sends a set of attribute values

indicating attributes of its own to said key management server; and said key

management server generates said attribute secret keys unique to said user terminal

based on, among said secret keys managed by said key management server, secret

keys corresponding to the attribute values sent from said user terminal and sends said

attribute secret keys to said user terminal (Matsumoto, Col. 4 Lines 37 – 49).

9.   As per claim 4, Matsumoto as modified teaches a key storage for storing secret

keys and public keys corresponding to predetermined attribute values; an attribute

secret key generator for obtaining a set of given attribute values and generating

attribute secret keys corresponding to said set of attribute values based on secret keys

corresponding to said attribute values among said secret keys stored in said key

storage (Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), and a

sending/receiving unit for receiving said set of attribute values from a given user

terminal and sending said attribute secret keys generated by said attribute secret key

generator to said user terminal (Matsumoto, Col. 4 Lines 57 – 67) wherein said attribute

values identifying said user terminal (Lerner, Col. 6 Lines 52 – 62).

10.   As per claim 6, Matsumoto teaches an encrypted content generator for

encrypting said content based on said criteria keys (Matsumoto, Col. 9 Lines 45 – 65)

and a sending unit for sending said encrypted content without specifying any recipient of

said content via a network (Matsumoto, Col. 4 Lines 57 – 67) but fails to teach a criteria

key generator for obtaining public keys corresponding to attribute values indicating

attributes of a recipient to which a content is to be sent and using said public keys to

generate criteria keys that can be decrypted by secret keys corresponding to said public

keys. However, in an analogous art Lerner teaches a criteria key generator for

obtaining public keys corresponding to attribute values indicating attributes of a recipient

to which a content is to be sent and using said public keys to generate criteria keys that

can be decrypted by secret keys corresponding to said public keys (Lerner, Col. 6 Lines

52 – 62).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Lerner's dynamic private key security with Matsumoto's

key management server and chat system because it offers the advantage of secure

messaging to secure privacy (Lerner, Col. 2 Lines 21 – 27).

11.   As per claim 7, Matsumoto teaches criteria key generator combines, based on

predetermined rules, criteria keys corresponding to the individual attribute values

encrypted by using public keys corresponding to said individual attribute values to

generate a criteria key for restricting recipients of said content (Matsumoto, Col. 4 Lines

37 – 49).

12.   As per claim 8, Matsumoto disclose criteria key generator generates a session

key for encrypting said content and a criteria key for decrypting said session key; and

said encrypted content generator uses said session key to encrypt said content content

(Matsumoto, Col. 4 Lines 37 – 49).

13.   As per claim 9, Matsumoto teaches a sending/receiving unit for accessing a key

management server managing (Matsumoto, Col. 4 Lines 57 – 67) and a decryptor for

obtaining an encrypted content and decrypting said content based on said attribute

secret keys (Matsumoto, Col. 11 Lines 2 – 8) but fails to teach secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys. However, in an analogous art Lerner teaches teach secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys (Lerner, Col. 6 Lines 52 – 62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Lerner's dynamic private key security with Matsumoto's key management server and chat system because it offers the advantage of secure messaging to secure privacy (Lerner, Col. 2 Lines 21 – 27).

14.   As per claim 10, Matsmoto teaches sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secrete keys generated based on said set of attribute values from said key management server (Matsumoto, Col. 4 Lines 37 – 49).

15.   Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto U.S. Patent No. (6,215,877) and Lerner et al. U.S. Patent No. (6,169,802), as applied to claim 1 and in further view of Kawano et al. U.S. Patent No. (5,933,605).

16.   As per claim 2, Matsumoto fails to teach provider terminal distributes said

encrypted content without specifying said user terminal that is to receive said encrypted

content. However, in an analogous art Kawano teaches provider terminal distributes

said encrypted content without specifying said user terminal that is to receive said

encrypted content (Kawano, Col.11 Lines 40 – 57).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Kawano's apparatus for filtering multicast messages with

Matsumoto's key management server and chat system because it offers the advantage

of have the data receiving operation that is not dependent on an expansion system

(Kawano, Col.11 Lines 40 – 57).

17.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Matsumoto U.S. Patent No. (6,215,877) and Lerner et al. U.S. Patent No. (6,169,802),

and in view of Applicant Admittance Prior Art (hereafter AAPA).

18.   As per claim 5, Matsumoto in view of Lerner fails to teach attribute secret key

generator generates said attribute secret keys by using a protocol implementing

oblivious transfer protocol. However, attribute secret key generator generates said

attribute secret keys by using a protocol implementing oblivious transfer is taught by

applicant on pages 14 and 15. The specification describes oblivious transfer protocol,

in order to be used secretly obtain attribute secret keys.

19.   Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Matsumoto U.S. Patent No. (6,215,877) in view of Applicant Admittance Prior Art

(hereafter AAPA) and Mooney et al. U.S. Patent No. (5,610,981).

20.   As per claim 19, Matsumoto teaches generating n secret keys and n public keys

corresponding to said secret keys and storing said secret keys and public keys in a

given storage, obtaining information about k (<=n) secret keys selected at random by a

given client from among said n secret keys stored in said storage; reading said k secret

keys corresponding to information about the obtained secret keys from said storage

(Matsumoto, Col. 2 Lines 60 – 67 and Col. 3 Lines 1 – 5), and providing said generated

decryption keys to said client (Matsumoto, Col. 4 Lines 57 – 67) but fails to teach using

a protocol for implementing oblivious transfer to generate decryption keys for decrypting

information encrypted with said k public keys corresponding to the k secret keys and

wherein n is the number of secret keys and public keys, and k is the number of the

secret keys selected at random by the given client. However, teach using a protocol for

implementing oblivious transfer to generate decryption keys for decrypting information

encrypted with said k public keys corresponding to the k secret keys is taught by

applicant on pages 14 and 15. The specification describes oblivious transfer protocol,

in order to be used secretly obtain attribute secret keys. Further, in an analogous art

Mooney teaches wherein n is the number of secret keys and public keys, and k is the

number of the secret keys selected at random by the given client (Mooney, Col. 14

Lines 36 – 50).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Mooney's preboot protection for a data security system

with Matsumoto's key management server and chat system because it offers the

advantage of securing physical access to a computer system (Mooney, Col. 1 Lines 31

– 37).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Roderick Tolentino whose telephone number is (571)

272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2134

Roderick Tolentino

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER